AMENDMENTS TO THE CLAIMS:

Please amend claims 1-37 and add newly written claims 38-43 as follows.

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method for computer security to control access to data held on a computer system as requestable datasets, ~~characterised in that it includes~~ said method comprising the steps of:

allocating computer system users between a plurality of user groups, each user group corresponding to a respective data access category selected from a plurality of such categories;

associating each dataset with a dataset access category; and

giving access to each dataset only to user group members associated with an appropriate data access category for that dataset.

2. (currently amended) A method according to Claim 1, wherein ~~characterised in that~~ the user groups and data access categories have hierarchical levels in which a higher data access category incorporates a or as the case may be each lower data access category, and the method includes allowing access to datasets by members of user groups associated with data access category levels equal to and higher than those to which such datasets correspond.

3. (currently amended) A method according to Claim 1, wherein ~~characterised in that~~ each user is associated with a computer-based identifying means and the method includes the step determining a user's identity from the identifying means.

4. (currently amended) A method according to Claim 3, wherein ~~characterised in that~~ the computer-based identifying means is an X.509 certificate.

5. (currently amended) A method according to Claim 1, wherein ~~characterised in that~~ the datasets are web pages and the method includes the step of gaining access to the computer network via the Internet or the World-Wide-Web.

6. (currently amended) A method according to Claim 1, wherein ~~characterised in that~~ the datasets are web pages and the step of associating each dataset with a dataset access category comprises inserting meta tags in html web page code.

7. (currently amended) A method according to Claim 1, further including ~~characterised in that it includes~~ the step of performing a challenge-response exchange regarding user identification before the step of giving access to a dataset.

8. (currently amended) A method according to Claim 1 in which a user employs a user computer system to gain access to datasets to which access is controlled by an access control computer system having a public key for verifying signed data, ~~characterised in that~~wherein each user computer system incorporates a private key for signing data and user group identifying means and the dataset access step includes:

using the private key to sign test data provided by the access control computer system and forwarding the signed data and identifying means to the access control computer system;

using the access control computer system to

verify the identifying means,

verify the user by using the public key to verify the signed data, and

determine user group and associated data access category from the identifying means.

9. (currently amended) A method according to Claim 8, wherein ~~characterised in that~~ the test data is random data.

10. (currently amended) A method according to Claim 1, further including the step of ~~characterised in that it includes~~ providing database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

11. (currently amended) A method according to Claim 1, wherein ~~characterised in that~~ data is maintained on ~~a~~at least one database computer system, dataset access is given by access control software ~~is~~ operated on a separate access control computer system, and a user gains access to data by means of access request software running on a user computer system separate from the database and access control computer systems.

12. (currently amended) A method according to Claim 11, wherein ~~characterised in that~~ the access control software is configured with a firewall protecting a database computer system.

13. (currently amended) A method according to Claim ~~11~~1, wherein ~~characterised in that~~ data is maintained on a plurality of database computer systems and in response to a data request ~~the~~ access control software determines whether or not corresponding data access is appropriate after relaying the request to a ~~dataset~~database computer system having such data.

14. (currently amended) A method according to Claim 1, wherein ~~characterised in that~~ data access categories and the user groups and datasets with which they are associated are assigned respective numerical values and the step of giving dataset access involves comparing user group and dataset numerical values to determine whether or not access is to be granted or denied.

15. (currently amended) A method according to Claim 14, wherein ~~characterised in that~~ the data access categories have different sections each with a section numerical value and the step of comparing numerical values comprises comparing section numerical values of corresponding sections of user group and dataset numerical values.

16. (currently amended) A method according to Claim 14, wherein ~~characterised in that~~ access to a dataset is provided only if all section comparisons are satisfied.

17. (currently amended) A method according to Claim 1, wherein ~~characterised in that~~ the step of giving access to a dataset includes unencrypted transfer of data from datasets to which access is granted.

18. (currently amended) A method according to Claim 16 wherein a user has a user computer system, wherein ~~characterised in that~~ the method includes the step of running checking/blocking software on the user computer system to screen incoming data for encryption to block unwanted data content.

19. (currently amended) A computer program product comprising a computer readable medium containing computer readable instructions for controlling operation of a computer system and providing control of access to data held on a computer system as requestable datasets, wherein ~~characterised in that~~ the computer readable instructions provide a means for controlling the computer system to~~program is arranged to~~:

~~(e)~~(a) receive data requests from computer system users allocated between a plurality of user groups, each user group corresponding to a respective data access category selected from a plurality of such categories;

~~(f)~~(b) control access to datasets each of which is associated with a dataset access category; and

~~(g)~~(c) give access to each dataset only to user group members associated with an appropriate data access category for that dataset.

20. (currently amended) A computer program product according to Claim 19, wherein ~~characterised in that~~ the user groups and data access categories have hierarchical levels in which a higher data access category incorporates a or as the case may be each lower data access category, and the computer readable instructions~~program is arranged to~~ allow access to datasets

by members of user groups associated with data access category levels equal to and higher than those to which such datasets correspond.

21. (currently amended) A computer program product according to Claim 19, wherein the computer readable instructions ~~characterised in that it is arranged to determine~~provide a means for determining a user's identity from computer-based identifying means.

22. (currently amended) A computer program product according to Claim 21, wherein ~~characterised in that~~ the computer-based identifying means is an X.509 certificate.

23. (currently amended) A computer program product according to Claim 19, wherein ~~characterised in that~~ the datasets are web pages and the computer readable instructions ~~program~~ enable~~s~~ access to the web pages via the Internet or the World-Wide-Web.

24. (currently amended) A computer program product according to Claim 19, wherein ~~characterised in that~~ the datasets are web pages and the computer readable instructions ~~program is arranged to identify~~provide a means for identifying dataset access categories in web pages from meta tags in html web page code.

25. (currently amended) A computer program product according to Claim 19, wherein ~~characterised in that it is arranged to~~computer readable instructions ~~challenge~~provide a means for challenging incoming data requests regarding user identification before giving access to a dataset.

26. (currently amended) A computer program product according to Claim 19 for interacting with a user computer system incorporating a private key for signing data and user group identifying means, the computer readable instructions provide a means for controlling the computer system~~program being arranged~~ to:

~~f)~~(d) send test data to the user computer system for signature with the private key and return with the identifying means,

~~g)~~(e) verify the identifying means,

~~h)~~(f) verify the user by using the public key to verify the signed data, and

~~i)~~(g) determine user group and associated data access category from the identifying means.

27. (currently amended) A computer program product according to Claim 26, wherein ~~characterised in that~~ the test data is random data.

28. (currently amended) A computer program product according to Claim 19, wherein the computer readable instructions ~~characterised in that it is arranged to~~ provide database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

29. (currently amended) A computer program product according to Claim 19, wherein the computer readable instructions ~~characterised in that it is arranged to~~ provide a firewall for a database computer system.

30. (currently amended) A computer program product according to Claim 19, wherein ~~characterised in that~~ data access categories and the user groups and datasets with which they are associated are assigned respective numerical values and the computer readable instructions provide a means for granting or denying~~program grants or denies~~ dataset access on the basis of comparison of user group and dataset numerical values.

31. (currently amended) A computer program product according to Claim 19, wherein the computer readable instructions provide a means for transferring ~~characterised in that it is arranged to transfer~~ dataset material to appropriate recipients unencrypted.

32. (currently amended) A network access controller for controlling access to data held on a computer system as requestable datasets, wherein ~~characterised in that~~ the controller ~~is arranged to~~:

~~f)~~(a) receives data requests from computer system users allocated between a plurality of user groups, each user group corresponding to a respective data access category selected from a plurality of such categories;

~~g)~~(b) controls access to datasets each of which is associated with a dataset access category; and

~~h)~~(c) gives access to each dataset only to user group members associated with an appropriate data access category for that dataset.

33. (currently amended) A controller according to Claim 32, wherein the controller ~~characterised in that it is adapted to~~ compares numerical values associated with data access categories of datasets and user groups in order to determine whether or not to grant access to data.

34. (currently amended) A controller according to Claim 32, wherein said controller ~~characterised in that it is arranged to~~ provides database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

35. (currently amended) A computer network for database access by users allocated between a plurality of user groups and having identifying certificates, wherein said network~~characterised in that it is arranged to~~ treats each user group as corresponding to a respective data access category selected from a plurality of such categories, and ~~it~~ includes:

~~f)~~(a) an access controller controlling access to a database comprising a plurality of datasets each having an associated dataset access category,

~~g)~~(b) means for verifying users,

~~h)~~(c) a database of datasets each of which is associated with a dataset access category; and

~~i)~~(d) computer software arranged to give access to each dataset only to user group members associated with an appropriate data access category for that dataset.

36. (currently amended) A network according to Claim 35, whereinecharacterised in the database comprises web pages in which dataset access categories are implemented by insertion of meta tags in web page html code.

37. (currently amended) A network according to Claim 35, wherein said network characterised in that it is an Internet or World-Wide Web network.

38. (new) A method for controlling user access to data held on a computer system as requestable datasets, the method including:

labelling the datasets with dataset access labels defining a hierarchy of data access levels,

allocating computer system users between a plurality of user groups,

labelling user groups with data access levels selected from a plurality of such levels; and

giving access to a requested dataset to a requesting member of a user group labelled with a data access level which in the hierarchy is equal to or above the data access level of the requested dataset.

39. (new) A method according to claim 38 wherein the datasets are web pages with dataset access labels which are meta tags, and a proxy server is used to:

receive requests for web pages from members of user groups,

check user group data access levels against a prearranged access control list, and

deny members of a user group access to requested web pages if they lack a data access level appearing on the access control list.

40. (new) A method for controlling user access to data held on a computer system as requestable web pages, the method including:

(a) labelling the web pages with meta tags defining a hierarchy of data access levels for an access control list,

(b) allocating computer system users between a plurality of user groups as members thereof, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) labelling user groups with respective data access levels associated with member groupings;

(d) using a proxy server to:

receive a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group,

send data for signature to the client computer system and obtain the requesting member's certificate,

receive data from the client computer system,

verify that the received data is:

(1) signed with the requesting member's key,

(2) a signed equivalent of the data sent to the requesting member for signature, and

(3) signed with a key from a certificate which is not time expired or invalid,

if the received data is verified as aforesaid, check the data access level of the requesting member's user group against the access control list, and

give access to a requested web page to the requesting member if it is a member of a user group labelled with a data access level which in the hierarchy is equal to or above the data access level of the requested web page.

41. (new) A network access control system for controlling access to data held on a computer system as requestable datasets, the control system being arranged to:

(a) label the datasets with dataset access labels defining a hierarchy of data access levels,

(b) communicate with computer system users allocated between a plurality of user groups,

(c) label user groups with data access levels selected from a plurality of such levels; and

(d) give access to a requested dataset to a requesting member of a user group labelled with a data access level which in the hierarchy is equal to or above the data access level of the requested dataset.

42. (new) A network access control system according to claim 41 wherein the datasets are web pages with dataset access labels which are meta tags and the control system has a proxy server for:

(e) receiving requests for web pages from members of user groups,

(f) checking user group data access levels against a prearranged access control list, and

(g) denying members of a user group access to requested web pages if they lack a data access level appearing on the access control list.

43. (new) A network access control system for controlling user access to data held on a computer system as requestable web pages, the control system being arranged to:

(a) label the web pages with meta tags defining a hierarchy of data access levels for an access control list,

(b) communicate with computer system users allocated between a plurality of user groups as members thereof, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) label user groups with respective data access levels associated with member groupings;

and the control system has a proxy server for:

(i) receiving a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group,

(ii) sending data for signature to the client computer system and obtain the requesting member's certificate,

(iii) receiving data from the client computer system,

(iv) verifying that the received data is:

(1) signed with the requesting member's key,

(2) a signed equivalent of the data sent to the requesting member for signature, and

(3) signed with a key from a certificate which is not time expired or invalid,

(v) if the received data is verified as aforesaid, checking the data access level of the requesting member's user group against the access control list, and

(vi) giving access to a requested web page to the requesting member if it is a member of a user group labelled with a data access level which in the hierarchy is equal to or above the data access level of the requested web page.